



Universal Serial Bus (USB) Checklist for Sharing Peripherals Across the Network (SPAN) Security Technical Implementation Guide Version 1 Release 1

06 January 2006

Developed by DISA for the DOD

Database Reference Number:		CAT I:
Database entered by:	Date:	CAT II:
Technical Q/A by:	Date:	CAT III:
Final Q/A by:	Date:	CAT IV:
		Total:

FOUO UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist Confidential System = CONFIDENTIAL Checklist Secret System = SECRET Checklist Top Secret System = SECRET Checklist

Enclave R	eviewer			Phone				
Previous S	SRR	Y N	Date of Previous SRR		S01 A	vailable	Y	N
Number of	f Current (Open Findin	gs					
G.1								
Site								
Name								
Address								
Phone								

Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				

USB00.001.00	CAT: 3	USB Powe	eroff Directi	ve in	SFUG							
8500.2 IA Control:	PRRB-1		Ca	tegory:	6.4 - Trai	ning & Ce	ertificati	ion				
Condition(s):												
Target(s):												
Vulnerability	There is no documer	nt instructing users	that USB devices I	be powe	red off for	at least 6	60 seco	nds prior	to being	connec	ted to an	IS.
	Because USB device means of maintaining 60 seconds when dis dissipate and the me The IAO will ensure prior to being connect	g memory for short sconnecting them fr mory erased. that the SFUG or a	power interruption om one IS, and co	s. Users	s need to e g to a differ	ensure the rent IS to	at USB make s	devices sure eno	remain v ugh time	vithout popularies	ower for a for all po	at least wer to
References:	SHARING PERIPHE	RALS ACROSS TH	IE NETWORK SE	CURITY	TECHNIC	CAL IMPL	LEMEN	TATION	GUIDE			
Checks:	SPAN USB00.001.00 documented that use allow all power to dis	ers should remove a	all power from a US									onds to
Fix(es):	SPAN USB00.001.0	0: Update the SFU	G, or an equivalen	t docum	ent, to incl	lude this i	informa	ition.				
OPE	N: NO	Γ A FINDING	: NO	T RE	VIEWE	D: [NOT	APPL	.ICAB	LE:	
Notes:												
USB01.001.00	CAT: 2	USB MP3	Players Car	mcore	ders ar	nd dig	gital d	camer	as			
USB01.001.00 8500.2 IA Control:		USB MP3	•		ders ar			camer	ras			
		USB MP3	•					camer	ras			
8500.2 IA Control:		USB MP3	•					camer	ras			
8500.2 IA Control: Condition(s): Target(s):			Ca	tegory:	2.1 - Obje	ect Permi	issions		ras			
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	DCBP-1	rders, or digital can in non-volatile men sensitive data lead ed to a DOD asset.	Ca neras are being att nory and could be a ng to the compron	ached to used to inise of the	2.1 - Obje o ISs witho infect an IS ne data. F	ect Permi out prior D S which the inally the	DAA app hey are	oroval. attached ormally no	d with ma o DOD re	equireme	ent for the	ese
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	DCBP-1 MP3 players, camco These devices conta be used to transport devices to be attache	rders, or digital can in non-volatile men sensitive data lead ed to a DOD asset. er will ensure that N	Caneras are being attemory and could be ong to the compronute MP3 players, came	ached to used to inise of the	2.1 - Obje o ISs witho infect an IS ne data. F or digital c	ect Permi out prior E S which the finally the	DAA app hey are ere is no are not a	oroval. attached ormally no attached	d with ma o DOD re to ISs w	equireme	ent for the	ese
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	MP3 players, camco These devices conta be used to transport devices to be attache The IAO, SA, and us	rders, or digital cam in non-volatile men sensitive data lead ed to a DOD asset. er will ensure that I RALS ACROSS TH	Can neras are being att nory and could be a ng to the compron MP3 players, camo HE NETWORK SE I interview the IAO	ached to used to inise of the corders, CURITY	2.1 - Object of ISs without infect an IS ne data. For digital control of TECHNIC that the IA	ect Permi out prior D S which the cameras a CAL IMPL AO know	DAA apphey are ere is not are not a LEMEN'	oroval. attachec ormally no attached TATION JSB devid	d with ma o DOD re to ISs w GUIDE ces such	equireme ithout pri as MP3	ent for the for DAA a players,	ese approval.
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	MP3 players, camco These devices conta be used to transport devices to be attache The IAO, SA, and us SHARING PERIPHE SPAN USB01.001.00 camcorders, or digita	rders, or digital camin non-volatile memsensitive data leaded to a DOD asset. er will ensure that Nata CRALS ACROSS The reviewer will all cameras are not to the IAO will be accompanion.	can being attorners are being attorners are being attorners and could be ong to the compronous MP3 players, camed RE NETWORK SEI interview the IAO to be attached to Ismade aware of the	ached to used to inise of the corders, CURITY to verify Ss without	2.1 - Object of ISs without on ISs without on ISs without or digital correction or digital correction or digital correction of that the IA without or on ISS defined that USB defined the IA without or on ISS defined the IA without or on ISS defined the IA without or on ISS defined the I	ect Permi out prior E S which the cameras a CAL IMPL AO know AA approv	DAA apphey are is not are not a LEMEN' vs that L val, and	attached attached attached TATION JSB devid I that this	d with map of DOD restor ISs with GUIDE ces such informations of the control of t	equirement ithout print as MP3 tion is dis corders,	ent for the for DAA a players, sseminate	ese approval. ed to all
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	MP3 players, camco These devices conta be used to transport devices to be attache The IAO, SA, and us SHARING PERIPHE SPAN USB01.001.00 camcorders, or digita users. SPAN USB01.001.00 cameras are not to b	rders, or digital camin non-volatile memsensitive data leaded to a DOD asset. er will ensure that Nata CRALS ACROSS The reviewer will all cameras are not to the IAO will be accompanion.	neras are being attenory and could be an one to the compronormal players, came the NETWORK SET interview the IAO to be attached to Is made aware of the ithout prior DAA and an one to the second seco	ached to used to inise of the corders, CURITY to verify Ss without	2.1 - Object of ISs without on ISs without on ISs without or digital correction or digital correction or digital correction of that the IA without or on ISS defined that USB defined the IA without or on ISS defined the IA without or on ISS defined the IA without or on ISS defined the I	ect Permi	DAA apphey are is not are not a LEMEN' vs that L val, and	oroval. attachecormally no attached TATION JSB device I that this MP3 playethe police	d with map of DOD restor ISs with GUIDE ces such informations of the control of t	equirement as MP3 tion is discorders, sers.	ent for the for DAA a players, sseminate or digital	ese approval. ed to all

USB01.002.00	CAT: 2	USB Devices Without Prior Approval	
8500.2 IA Control:	DCBP-1	Category: 12.4 - CM Process	
Condition(s):			
Target(s):			
Vulnerability	USB devices are atta	ched to a DOD IS without prior IAO approval.	
	being attached. By re	aware of what type of USB devices are being attached to DOD ISs and needs to stop prohibited devices from equiring the IAO to approve the USB devices the IAO will be informed. Issure that no USB device is attached to a DOD IS unless approved by the IAO.	
References:	SHARING PERIPHEI	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE	
Checks:		: The reviewer will interview the IAO or SA to verify that prior approval by the IAO is required before USB device ISs and that this policy is disseminated to all users.	es
Fix(es):	IAO will ensure that the	: The IAO will know that approval by the IAO is required before USB devices are attached to DOD ISs and the nis policy is disseminated to all users.	
OPE		A FINDING: NOT REVIEWED: NOT APPLICABLE:	
Notes:			_
USB01.003.00	CAT: 2	USB Disguised Jump Drives	
USB01.003.00 8500.2 IA Control:	_	USB Disguised Jump Drives Category: 5.9 - Device Locations	
	_	·	
8500.2 IA Control:	_	·	
8500.2 IA Control: Condition(s): Target(s):	DCBP-1	·	
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	DCBP-1 Disguised jump drive: Since they could easi location, disguised Us	Category: 5.9 - Device Locations	
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	DCBP-1 Disguised jump drives Since they could easi location, disguised Ut The IAO, SA, and use	Category: 5.9 - Device Locations s are not banned from locations containing DOD ISs. ly be overlooked in a spot search to verify that no restricted or sensitive information is being removed from a SB jump drives will be banned from locations containing DOD ISs.	
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	DCBP-1 Disguised jump drive: Since they could easi location, disguised U: The IAO, SA, and use SHARING PERIPHEI SPAN USB01.003.00	Category: 5.9 - Device Locations s are not banned from locations containing DOD ISs. ly be overlooked in a spot search to verify that no restricted or sensitive information is being removed from a SB jump drives will be banned from locations containing DOD ISs. er will ensure disguised jump drives are not permitted in locations containing DOD ISs.	
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	DCBP-1 Disguised jump driver. Since they could easi location, disguised Ut The IAO, SA, and use SHARING PERIPHEL SPAN USB01.003.00 containing DOD ISs is	Category: 5.9 - Device Locations s are not banned from locations containing DOD ISs. lly be overlooked in a spot search to verify that no restricted or sensitive information is being removed from a SB jump drives will be banned from locations containing DOD ISs. er will ensure disguised jump drives are not permitted in locations containing DOD ISs. RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 1: The reviewer will interview the IAO to verify that the policy banning disguised jump drives from locations	
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	DCBP-1 Disguised jump driver. Since they could easi location, disguised USThe IAO, SA, and use SHARING PERIPHEI SPAN USB01.003.00 containing DOD ISs is SPAN USB01.003.00	Category: 5.9 - Device Locations s are not banned from locations containing DOD ISs. ly be overlooked in a spot search to verify that no restricted or sensitive information is being removed from a SB jump drives will be banned from locations containing DOD ISs. er will ensure disguised jump drives are not permitted in locations containing DOD ISs. RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 1: The reviewer will interview the IAO to verify that the policy banning disguised jump drives from locations is disseminated to all users. 2: Disseminate the policy banning disguised jump drives from locations containing DOD ISs to all users.	

USB01.004.00	CAT: 2	USB Notice of Disguised Jump Drive Ban
8500.2 IA Control:	DCBP-1	Category: 11.6 - Warning Banners
Condition(s):		
Target(s):		
Vulnerability	Notices are not prom	inently displayed informing everyone of the ban of disguised jump drives.
Vulnerability Discussion:	Without a notice bein	g posted, users could violate the ban and protest the seizer of the devices.
References:	SHARING PERIPHE	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:	SPAN USB01.004.00): The reviewer will interview the IAO and view the notices.
Fix(es):	SPAN USB01.004.00 drives are banned	2: Post the required notices informing people entering a location containing DOD ISs that disguised USB jump
OPE	N: NOT	A FINDING: NOT REVIEWED: NOT APPLICABLE:
Notes:		
Condition(s):	CAT: 2 PECS-1: PECS-2: PE	USB Persistent Memory DODD 5200-1-R Treatment EDD-1 Category: 11.4 - Disposition
Target(s): Vulnerability		SB devices are not treated as removable media and contrary to DODD 5200.1-R; the devices are not secured, itized in a manner appropriate for the classification level of the data they contain.
	capacity. They will be level of the data they The IAO, SA, and use	SB devices can function as removable media. They have the same vulnerabilities as floppy disk but greater e secured, transported and sanitized as required by DODD 5200-1-R in a manner appropriate for the classification contain. er will ensure that persistent memory USB devices are treated as removable media and, in accordance with DODD is are secured, transported, and sanitized in a manner appropriate for the classification level of the data they
References:	SHARING PERIPHE	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:	removable media, an appropriate for the cla	2: The reviewer will interview the IAO to verify that the policy for treating persistent memory USB devices as id in accordance with DODD 5200.1-R; the devices are secured, transported, and sanitized in a manner assification level of the data they contain is disseminated to all users. This would include any device with internal stent memory not just jump drives or disk driver.
Fix(es):	in accordance with D	D: Disseminate the policy requiring that persistent memory USB devices will be treated as removable media and, ODD 5200.1-R; the devices will be secured, transported, and sanitized in a manner appropriate for the the data they contain.
OPE	N: NOT	A FINDING: NOT REVIEWED: NOT APPLICABLE:
Notes:		

USB01.006.00	CAT: 2	Persistent Memory USB Devices Labeled
8500.2 IA Control:	ECML-1	Category: 11.5 - Device Labels
Condition(s):		
Target(s):		
Vulnerability	Persistent memory U	ISB devices are not labeled in accordance with the classification level of the data they contain.
		nory USB device is not labeled with the appropriate classification level this can lead to the compromise of sensitive ise of an IS that the device is attached.
References:	SHARING PERIPHE	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:		D: The reviewer will interview the IAO or SA to verify that the labeling of persistent memory USB devices is in classification level of the data they contain.
Fix(es):	SPAN USB01.006.00 Disseminate this poli	D: Label persistent memory USB devices in accordance with the classification level of the data they contain. cy to all users.
ОРЕ	N: NOT	A FINDING: NOT REVIEWED: NOT APPLICABLE:
Notes:		
USB01.007.00	CAT: 2	Unanamental Canaitive Data
	CAI.Z	Unencrypted Sensitive Data
8500.2 IA Control:	_	Unencrypted Sensitive Data Category: 8.2 - Encrypted Data at Rest
8500.2 IA Control: Condition(s):	_	Category: 8.2 - Encrypted Data at Rest
8500.2 IA Control: Condition(s): Target(s):	_	• •
Condition(s): Target(s):	ECCR-1: ECCR-2	Category: 8.2 - Encrypted Data at Rest d on a USB device with persistent memory, that the data owner requires encryption is not encrypted using NIST-
Condition(s): Target(s): Vulnerability Vulnerability	Sensitive data stored certified cryptograph; If the data owner beli compromise of sensi The IAO, SA, and us	Category: 8.2 - Encrypted Data at Rest d on a USB device with persistent memory, that the data owner requires encryption is not encrypted using NIST- y. ieves that the data requires encryption it will be encrypted when at rest. If it is not encrypted this can lead to the
Condition(s): Target(s): Vulnerability Vulnerability Discussion:	Sensitive data stored certified cryptography If the data owner beli compromise of sensi The IAO, SA, and us is encrypted using N	Category: 8.2 - Encrypted Data at Rest d on a USB device with persistent memory, that the data owner requires encryption is not encrypted using NIST- y. ieves that the data requires encryption it will be encrypted when at rest. If it is not encrypted this can lead to the tive data. er will ensure that all sensitive data stored on a USB device with persistent memory, if required by the data owner,
Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	Sensitive data stored certified cryptograph: If the data owner beli compromise of sensit The IAO, SA, and us is encrypted using N SHARING PERIPHE SPAN USB01.007.00	Category: 8.2 - Encrypted Data at Rest d on a USB device with persistent memory, that the data owner requires encryption is not encrypted using NIST- y. ieves that the data requires encryption it will be encrypted when at rest. If it is not encrypted this can lead to the tive data. er will ensure that all sensitive data stored on a USB device with persistent memory, if required by the data owner, IST-certified cryptography.
Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	Sensitive data stored certified cryptography If the data owner beli compromise of sensi The IAO, SA, and us is encrypted using N SHARING PERIPHE SPAN USB01.007.00 memory, if required to SPAN USB01.007.00	Category: 8.2 - Encrypted Data at Rest d on a USB device with persistent memory, that the data owner requires encryption is not encrypted using NIST- y. ieves that the data requires encryption it will be encrypted when at rest. If it is not encrypted this can lead to the tive data. er will ensure that all sensitive data stored on a USB device with persistent memory, if required by the data owner, IST-certified cryptography. ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE O: The reviewer will interview the IAO to verify that all sensitive data stored on a USB device with persistent by the data owner, is encrypted using NIST-certified cryptography. O: Establish a process that will disseminate the requirement for encrypt of sensitive data that the data owner ng encryption. Also establish a process identifying which data needs to be encrypted and notifying the users that
Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	Sensitive data stored certified cryptograph: If the data owner belicompromise of sensitive IAO, SA, and us is encrypted using N SHARING PERIPHE SPAN USB01.007.00 memory, if required by SPAN USB01.007.00 designates as needing the identified data ne	Category: 8.2 - Encrypted Data at Rest d on a USB device with persistent memory, that the data owner requires encryption is not encrypted using NIST- y. ieves that the data requires encryption it will be encrypted when at rest. If it is not encrypted this can lead to the tive data. er will ensure that all sensitive data stored on a USB device with persistent memory, if required by the data owner, IST-certified cryptography. ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE O: The reviewer will interview the IAO to verify that all sensitive data stored on a USB device with persistent by the data owner, is encrypted using NIST-certified cryptography. O: Establish a process that will disseminate the requirement for encrypt of sensitive data that the data owner ng encryption. Also establish a process identifying which data needs to be encrypted and notifying the users that

USB01.008.00	CAT: 2	USB Format for Access Controls
8500.2 IA Control:	DCBP-1	Category: 2.1 - Object Permissions
Condition(s):		
Target(s):		
Vulnerability	USB devices with per the device.	ersistent memory are not formatted in a manner to allow the application of Access Controls to files or data stored on
	any system that the Note that access co encryption. The IAO, SA, and us	nat that allows the application of access controls to the device files stored on the USB device may be accessed from device is connected to. Introls are easily bypassed on USB devices so this should not be considered an adequate replacement for ser will ensure that USB devices with persistent memory are formatted in a manner to allow the application of iles or data stored on the device.
References:	SHARING PERIPHE	ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:		0: The reviewer will interview the IAO to verify that USB devices with persistent memory are formatted in a manner ion of Access Controls to files or data stored on the device. For devices used on a Windows system this would be
Fix(es):		0: Develop a process to disseminate the requirement that USB devices with persistent memory will be formatted in e application of Access Controls to files or data stored on the device.
OPE	N: NO	T A FINDING: NOT REVIEWED: NOT APPLICABLE:
Notes:		
140.00.		
USB01.009.00	CAT: 2	USB SFUG Section
USB01.009.00 8500.2 IA Control:	_	
	_	USB SFUG Section Category: 6.4 - Training & Certification
8500.2 IA Control:	_	
8500.2 IA Control: Condition(s): Target(s):	PRRB-1	
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	There is no section. The Security Feature procedures describin The reviewer will into of USB devices. Add	Category: 6.4 - Training & Certification
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	There is no section of the Security Feature procedures describing The reviewer will into of USB devices. Ad government owned	Category: 6.4 - Training & Certification within the SFUG, or equivalent documentation, describing the correct usage and handling of USB technologies. es User Guide gives the user a single reference for information on the current general and site policies and any their security responsibilities. The lack of this reference could lead to the compromise of sensitive data. Perview the IAO and review the relevant document. What needs to be here is a description for handling, and labeling ditionally an explanation of the restrictions placed on attaching non-government owned USB devices to a
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	There is no section of The Security Feature procedures describing The reviewer will introf USB devices. Ad government owned SHARING PERIPHE SPAN USB01.009.0 for handling, and lab	Category: 6.4 - Training & Certification within the SFUG, or equivalent documentation, describing the correct usage and handling of USB technologies. es User Guide gives the user a single reference for information on the current general and site policies and not their security responsibilities. The lack of this reference could lead to the compromise of sensitive data. erview the IAO and review the relevant document. What needs to be here is a description for handling, and labeling ditionally an explanation of the restrictions placed on attaching non-government owned USB devices to a IS and the prohibition of disguised USB jump drives.
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	There is no section of the Security Feature procedures describing The reviewer will into of USB devices. Ad government owned SHARING PERIPHE SPAN USB01.009.0 for handling, and lab USB devices to a go	Category: 6.4 - Training & Certification within the SFUG, or equivalent documentation, describing the correct usage and handling of USB technologies. es User Guide gives the user a single reference for information on the current general and site policies and ng their security responsibilities. The lack of this reference could lead to the compromise of sensitive data. erview the IAO and review the relevant document. What needs to be here is a description for handling, and labeling ditionally an explanation of the restrictions placed on attaching non-government owned USB devices to a IS and the prohibition of disguised USB jump drives. ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE O: The reviewer will interview the IAO and review the relevant document. What needs to be here is a description religing of USB devices. Additionally an explanation of the restrictions placed on attaching non-government owned
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	There is no section of the Security Feature procedures describing the reviewer will into of USB devices. Ad government owned SHARING PERIPHE SPAN USB01.009.0 for handling, and lab USB devices to a government owned sharing.	Category: 6.4 - Training & Certification within the SFUG, or equivalent documentation, describing the correct usage and handling of USB technologies. es User Guide gives the user a single reference for information on the current general and site policies and not their security responsibilities. The lack of this reference could lead to the compromise of sensitive data. erview the IAO and review the relevant document. What needs to be here is a description for handling, and labeling ditionally an explanation of the restrictions placed on attaching non-government owned USB devices to a IS and the prohibition of disguised USB jump drives. ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 0: The reviewer will interview the IAO and review the relevant document. What needs to be here is a description seling of USB devices. Additionally an explanation of the restrictions placed on attaching non-government owned overnment owned IS and the prohibition of disguised USB jump drives.
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks: Fix(es):	There is no section of the Security Feature procedures describing the reviewer will into of USB devices. Ad government owned SHARING PERIPHE SPAN USB01.009.0 for handling, and lab USB devices to a government owned sharing.	Category: 6.4 - Training & Certification within the SFUG, or equivalent documentation, describing the correct usage and handling of USB technologies. es User Guide gives the user a single reference for information on the current general and site policies and not their security responsibilities. The lack of this reference could lead to the compromise of sensitive data. Perview the IAO and review the relevant document. What needs to be here is a description for handling, and labeling ditionally an explanation of the restrictions placed on attaching non-government owned USB devices to a IS and the prohibition of disguised USB jump drives. ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE O: The reviewer will interview the IAO and review the relevant document. What needs to be here is a description peling of USB devices. Additionally an explanation of the restrictions placed on attaching non-government owned overnment owned IS and the prohibition of disguised USB jump drives. O: Develop, update, and distribute a SFUG section dealing with USB devices in accordance with the SPAN STIG.

USB01.010.00	CAT: 3	USB SFUG Persistent Non-Removable Memory
8500.2 IA Control:	PRRB-1	Category: 6.4 - Training & Certification
Condition(s):		
Target(s):		
Vulnerability	The USB usage secremovable memory.	tion of the SFUG, or equivalent document, does not contain a discussion of the devices that contain persistent non-
	device to an IS leadi Additionally the user a device.	of tthe devices that contain persistent non-removable memory, an uninformed user can mistakenly attach such a ng to the denial of service caused by an infection of the IS and possibly the network with malicious code. might compromise sensitive data thinking that removal of a memory card removed all the persistent memory within that the USB usage section of the SFUG contains a discussion of the devices that contain persistent non-
References:	SHARING PERIPHE	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:		0: The reviewer will interview the IAO and review the relevant documentation. The discussion should point out that may not be obvious that it contains persistent non-removable memory and that, if there is a doubt, it will be treated stent memory.
Fix(es):		0: Develop, update, and distribute a SFUG section on USB devices that discusses devices that may contain vable memory in accordance with the SPAN STIG.
OPE	N: NO	T A FINDING: NOT REVIEWED: NOT APPLICABLE:
Notes:		
USB02.011.00	CAT: 1	An IS BIOS Set to Allow Boot from USB
USB02.011.00 8500.2 IA Control:		An IS BIOS Set to Allow Boot from USB Category: 2.1 - Object Permissions
8500.2 IA Control:		
8500.2 IA Control: Condition(s): Target(s):	DCBP-1	
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	DCBP-1 An IS has its BIOS s If an IS's BIOS is left either performing a h	Category: 2.1 - Object Permissions
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	DCBP-1 An IS has its BIOS s If an IS's BIOS is left either performing a h denial of service. Act the IS is attached.	Category: 2.1 - Object Permissions et to allow a boot from a USB device. set to allow it to be booted from a USB device, an individual can plug a USB device into the IS and force a reboot, hardware reset or cycling the power, causing whatever operating system is on their USB device. This can lead to a
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	DCBP-1 An IS has its BIOS s If an IS's BIOS is left either performing a h denial of service. Ac the IS is attached. SHARING PERIPHE SPAN USB02.011.0	Category: 2.1 - Object Permissions et to allow a boot from a USB device. set to allow it to be booted from a USB device, an individual can plug a USB device into the IS and force a reboot, hardware reset or cycling the power, causing whatever operating system is on their USB device. This can lead to a diditionally this can lead to the compromise of sensitive data on the IS that was rebooted and possibly to the network
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	DCBP-1 An IS has its BIOS is left either performing a hidenial of service. Act the IS is attached. SHARING PERIPHE SPAN USB02.011.0 device. Note an IS in normal use. SPAN USB02.011.0	Category: 2.1 - Object Permissions et to allow a boot from a USB device. set to allow it to be booted from a USB device, an individual can plug a USB device into the IS and force a reboot, hardware reset or cycling the power, causing whatever operating system is on their USB device. This can lead to a additionally this can lead to the compromise of sensitive data on the IS that was rebooted and possibly to the network ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE O: The reviewer will interview the IAO or SA to verify that no IS has its BIOS set to allow a boot from any USB
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	An IS has its BIOS s If an IS's BIOS is left either performing a h denial of service. Ac the IS is attached. SHARING PERIPHE SPAN USB02.011.0 device. Note an IS in normal use. SPAN USB02.011.0 are set to allow a bo	Category: 2.1 - Object Permissions et to allow a boot from a USB device. set to allow it to be booted from a USB device, an individual can plug a USB device into the IS and force a reboot, nardware reset or cycling the power, causing whatever operating system is on their USB device. This can lead to a diditionally this can lead to the compromise of sensitive data on the IS that was rebooted and possibly to the network ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 0: The reviewer will interview the IAO or SA to verify that no IS has its BIOS set to allow a boot from any USB can be booted from a USB device for maintenance or recovery purposes, but will never be allowed to do so when 0: Develop a plan to check all ISs' BIOS settings as soon a possible. The check will verify that none of the BIOS
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks: Fix(es):	An IS has its BIOS s If an IS's BIOS is left either performing a h denial of service. Ac the IS is attached. SHARING PERIPHE SPAN USB02.011.0 device. Note an IS in normal use. SPAN USB02.011.0 are set to allow a bo	Category: 2.1 - Object Permissions et to allow a boot from a USB device. set to allow it to be booted from a USB device, an individual can plug a USB device into the IS and force a reboot, hardware reset or cycling the power, causing whatever operating system is on their USB device. This can lead to a diditionally this can lead to the compromise of sensitive data on the IS that was rebooted and possibly to the network ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 0: The reviewer will interview the IAO or SA to verify that no IS has its BIOS set to allow a boot from any USB can be booted from a USB device for maintenance or recovery purposes, but will never be allowed to do so when 0: Develop a plan to check all ISs' BIOS settings as soon a possible. The check will verify that none of the BIOS of from a USB device. Obtain CM approval for the plan and execute the plan.